BAB 5
SIMPULAN DAN SARAN

5.1 Simpulan

ZK-SNARK berhasil diimplementasikan pada modul autentikasi identitas pada sistem *E-voting* berbasis blockchain. Hal tersebut dapat dilihat dalam proses autentikasi yang diimplementasikan pada sistem yang tidak melibatkan data-data sensitif atau privat yang berhubungan dengan identitas seorang *voter*. Selain itu, *proof* yang dihasilkan juga bersifat *succinct* dan *non-interacive* sehingga proses autentikasi dapat menjadi lebih sederhana ketika dilakukan secara *off-chain* maupun *on-chain*. *Proof* pada ZK-SNARK dihasilkan dengan menggunakan *elliptic curve digital signature algorithm* (ECDSA) yang telah tersedia secara *native* pada blockchain Ethereum sehingga keamanan dari proses autentikasi telah teruji.

Performa dari sistem yang dibangun berhasil diuji dari sisi *throughput* dan skalabilitas dengan menggunakan metode *load testing*. Berdasarkan dua skenario yang telah dilakukan pada pengujian, *throughput* yang dihasilkan pada skenario 2 menghasilkan nilai *throughput* untuk masing-masing jumlah *host* lebih tinggi daripada yang dihasilkan pada skenario 1 karena skenario 2 tidak menggunakan *load balancer* dan tidak ada beban tambahan dari jaringan. Dari sisi *Speedup*, keduanya menghasilkan nilai yang semakin meningkat seiring dilakukannya penambahan jumlah *host*, namun secara garis besar tingkat kenaikan nilai *Speedup* tersebut semakin berkurang (sub-linear) seiring dilakukannya menambahan jumlah *host*. Sedangkan dari sisi efisiensi, keduanya mengalami penurunan seiring dilakukannya penambahan jumlah *host*.

Performa dari sistem juga berhasil diuji dari sisi biaya dengan cara mengukur *gas fee* dari operasi *on-chain* yang dilakukan, seperti meluncurkan *smart contract* ke jaringan blockchain dan menambahkan data identitas *voter* pada *smart contract*. Perbandingan juga berhasil dilakukan terhadap performa sistem dari sisi biaya jika menggunakan tiga jaringan blockchain yang berbeda, yaitu Ethereum Mainnet, Polygon, dan Arbitrum One. Jaringan blockchain Ethereum Mainnet memiliki biaya tertinggi, sedangkan jaringan Polygon dan Arbitrum One memiliki biaya yang rendah dan perbedaannya tidak signifikan.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan, terdapat beberapa saran agar sistem dapat ditingkatkan kembali di masa depan, antara lain:

- Pada penelitian ini, sistem yang dibangun hanya mencakup modul autentikasi dari sistem *E-voting* berbasis blockcain sehingga pengembangan sistem ke depannya dapat berfokus pada pembangunan modul dan mekanisme untuk pemberian suara pada proses *voting*.
- Metode autentikasi menggunakan ZK-SNARK dapat dipadukan dengan metode autentikasi lainnya seperti *biometric*, OTP, dan sebagainya menjadi *two-factor* atau *multi-factor authentication* untuk semakin memperketat keamanan sistem dan menghindari berbagai macam serangan seperti *man in the middle* (MiTM).
- Performa sistem yang dibangun dari sisi *throughput* dan skalabilitas pada dapat ditingkatkan kembali dengan memanfaatkan fitur *autoscaling* pada layanan *Cloud Computing* dari beberapa *provider* ternama, seperti Google Cloud, Amazon Web Service (AWS), Digital Ocean, Vercel, dan sebagainya. Dengan *autoscaling*, *provider* yang digunakan akan melakukan *scale up* atau *scale down* secara otomatis berdasarkan beban kerja yang diterima dan biaya yang paling optimal.